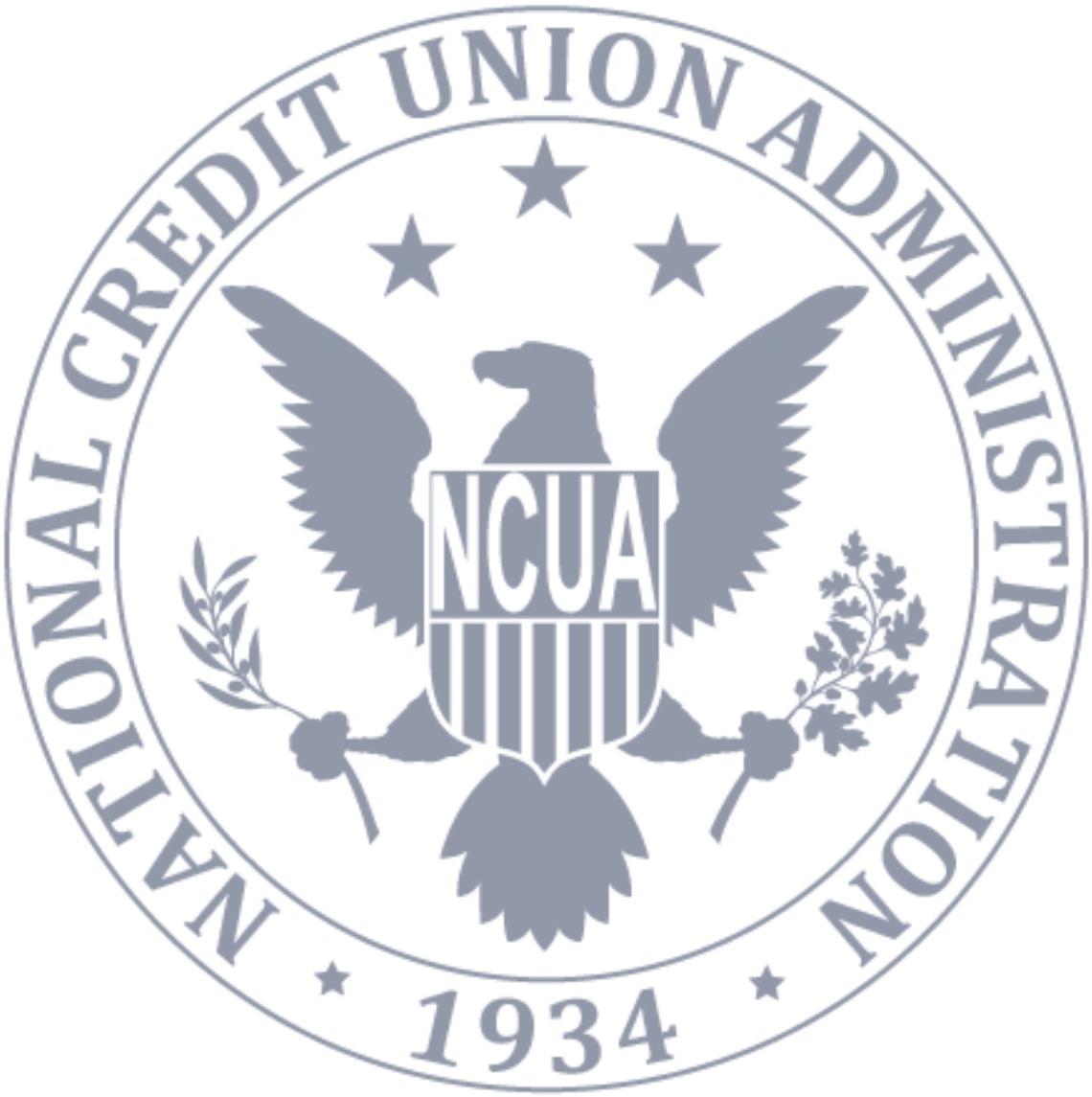
NCUA
National Credit Union Administration

Privacy Impact Assessment for ESS/MERIT

Fiscal Year 2022

[This page intentionally left blank]



About this Document

A Privacy Impact Assessment (PIA) is an analysis of how PII is handled to ensure that handling conforms to applicable privacy requirements, to determine the privacy risks associated with an information system or activity, and to evaluate ways to mitigate privacy risks. A PIA is both an analysis and a formal document detailing the process and the outcome of the analysis.

Program offices and system owners are required to complete a PIA whenever they develop, procure, or use information technology to create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII.[1] Completion of a PIA is a precondition for the issuance of an authorization to operate.[2]

Basic Information about the System

System Name: ESS/MERIT

NCUA Office of Primary Interest: Office of Business Innovation

Threshold		
1	*What is the status of the system/tool/application (for simplicity referred to as "system" going forward)?*	Operational
2	*Describe the system in 1-2 sentences.*	As the primary tool for NCUA's examination and supervision responsibilities, ESS/MERIT will be used by the NCUA and state examiners to review and analyze data related to the operations of federally insured credit unions and some state-chartered, non-federally insured credit unions. ESS/MERIT is based on the Metricstream Governance, Risk, and Compliance (GRC) commercial-off-the-shelf (COTS) solution. The system will aggregate

[1] 44 U.S.C. § 3501, note; Pub. L. 107–347, § 208(b).
[2] OMB Memorandum M-14-04, *Fiscal Year 2013 Reporting Instructions for the Federal Information Security Act and Agency Privacy Management* (2013).

		quarterly credit union reports that capture financial and operational data about credit unions, including information about credit union officials. The system will also facilitate the NCUA's review of individuals' credit union share and loan information. The system is being revised to add the recordings of meetings between individuals representing the NCUA and credit unions to the Categories of Records section.

Purpose and Authority

The NCUA should only create, collect, use, process, store, maintain, disseminate, or disclose PII if it has authority to do so, and such authority should be identified in the appropriate notice.

The NCUA should provide notice of the specific purpose for which PII is collected and should only use, process, store, maintain, disseminate, or disclose PII for a purpose that is explained in the notice and is compatible with the purpose for which the PII was collected, or that is otherwise legally authorized.

Purpose and Authority		
1	*What is the purpose of the system?*	ESS/MERIT will assist in accomplishing the NCUA's statutorily mandated examination and supervision activities, including the coordination and conduct of examinations, supervisory evaluations and analyses, enforcement actions and Federal court actions. NCUA may coordinate with other financial regulatory agencies on matters related to the safety and soundness of credit unions. The information collected in this system will also support the conduct of investigations or be used as evidence by the NCUA or other supervisory or law enforcement agencies. This may result in criminal referrals, referrals to Offices of Inspectors General, or the initiation of administrative or Federal court actions. This system will track and store examination and supervision documents created during the

		performance of the NCUA's statutory duties. The information will also be used for administrative purposes to ensure quality control, performance, and improving examination and supervision processes.
2	*How is the PII collected/maintained/used in the system relevant and necessary to achieve the purpose described above?*	NCUA intends to transform credit union examination and supervision processes and tools to enable proactive, risk-focused, data driven decisions and to enhance efficiency, security, and business agility. As the primary tool for NCUA's examination and supervision responsibilities, ESS/MERIT will be used by the NCUA and state examiners to review and analyze data related to the operations of federally insured credit unions and some state-chartered, non-federally insured credit unions.
3	*What is the legal authority to collect, maintain, use, or share the PII contained in the system?*	12 U.S.C. § 1751 et seq.

Minimization

The NCUA should only create, collect, use, process, store, maintain, disseminate, or disclose PII that is directly relevant and necessary to accomplish a legally authorized purpose, and should only maintain PII for as long as is necessary to accomplish that purpose.

The NCUA recognizes the increased sensitivity of Social Security numbers (SSNs) and therefore makes every effort to limit the collection and maintenance of them. The NCUA also limits its collection of other types of PII to those that are necessary.

SSNs		
1	*Will the system collect, maintain, or share social security numbers?*	• Yes
1.1	*Of who?*	• CU Members • CU Officers, Employees, Volunteers • Others: State Supervisory Authorities (SSAs)
1.2	*What is the law that authorizes this collection of SSNs?*	• 12 U.S.C. § 1751 et seq.

1.3	*Will the system collect, maintain, or share social security numbers?*	• To evaluate the safety and soundness of credit union practices related to their primary services to members: loans and shares.
1.4	*Why would using a less sensitive identifier or group of identifiers be insufficient*	• SSNs are an integral part of a credit union member's record. Further, SSNs help identify potential fraud in the credit union (confirm an individual's identity, duplicate SSN numbers, etc.).
1.5	*Approximately how many unique SSNs will be maintained in the system?*	• More than 100,000

PII		
1	*Basic Demographic*	• Email Address • First Name • Home Address • Last Name • Middle Name (or initial) • Phone Number • Other: Credit Union Service Organizations (CUSOs)
1.1	*Who is it collected for?*	• CU Members • CU Officers, Employees, Volunteers • NCUA Employees/Contractors
2	*Medical and Family*	• Information about Spouse(s), Children, or other Family Members • Marital Status or Marriage/Divorce Records
2.1	*Who is it collected for?*	• CU Members • CU Officers, Employees, Volunteers
3	*Financial*	• Account Number • Credit Score / Credit History • Credit Union Account Number • Financial Responsibility Determinations or Related Information • Loan and Share Information • Other: Business relationships (e.g. Business loan and the ownership of the business.)

3.1	*Who is this information collected for?*	• CU Members • CU Officers, Employees, Volunteers
4	*Biometric*	• Signature • Voice Recording • Other: Video recordings
4.1	*Who is this information collected for?*	• CU Members • CU Officers, Employees, Volunteers • NCUA Employees/Contractors
5	*Employment and Education*	• Current Employment Information other than NCUA Employment (such as Occupation, Employer, Work Address, Work Phone, Work Email, Title, Salary) • Education Information (including Professional Certifications) • Employment History • Employment Identification Number (EIN) • Other: CUSOs
5.1	*Who is this information collected for?*	• CU Members • CU Officers, Employees, Volunteers • NCUA Employees/Contractors
6	*Information Technology (IT)*	• Login/Activity Records
6.1	*Who is this information collected for?*	• CU Officers, Employees, Volunteers • NCUA Employees/Contractors • Others: SSAs
7	*NCUA Employment*	• NCUA Email Address • NCUA iPhone Number • NCUA Office Phone Number • Physical Movements (Key Entry records, Video, etc.) • Other: Voice recordings of NCUA employees
7.1	*Who is this information collected for?*	• NCUA Employees/Contractors

Collection and Consent

The NCUA should create, collect, use, process, store, maintain, disseminate, or disclose PII with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to ensure fairness to the individual.

The NCUA should involve the individual in the process of using PII and, to the extent practicable, seek individual consent for the creation, collection, use, processing, storage, maintenance, dissemination, or disclosure of PII. The NCUA should also establish procedures to receive and address individuals' privacy-related complaints and inquiries.

The NCUA endeavors both to collect information from the subject individual, and to attain affirmative informed consent, whenever possible. The NCUA's use of Privacy Act statements and privacy notices on forms are critical to this effort. For more information see the Transparency section below.

Collection and Consent		
1	*What are the sources from which the PII will be collected?*	• A Credit Union • Other: The information in the system about credit union officials and individual credit union members is generally provided by credit unions and CUSOs. NCUA employees and contractors, and State Supervisory Authorities may add additional information to the system as part of their assigned supervision and examination activities (including analytics/business intelligence activities). Some of the information may be from third parties with relevant information about covered persons or service providers, or existing databases maintained by other Federal and state regulatory associations, law enforcement agencies, and related entities. Whenever practicable, the NCUA collects information about an individual directly from that individual.

2	*How will the information be collected?*	• From another Information System • Web-based Form or Email • Other: The information in the system about credit union officials and individual credit union members is generally provided by credit unions and CUSOs. NCUA employees and contractors, and State Supervisory Authorities may add additional information to the system as part of their assigned supervision and examination activities (including analytics/business intelligence activities). Some of the information may be from third parties with relevant information about covered persons or service providers, or existing databases maintained by other Federal and state regulatory associations, law enforcement agencies, and related entities.
3	*Will the individuals whose information is collected/maintained in the system consent to their personal information?*	• Yes, the individuals affirmatively consent to providing the information for the purpose and uses described in this system.
4	*Will individuals be able to "opt-out" by declining to provide PII or by consenting only to a particular use?*	• No

Procedures to Address Individuals' Privacy Related Complaints and Inquiries

The Privacy team knows that complaints, concerns, and questions from individuals can be a valuable source of input that improves operational models, uses of technology, data collection practices, and privacy safeguards. To facilitate this type of feedback, the Privacy team has established the Privacy Complaint Process to receive and respond to complaints, concerns, and questions from individuals about the NCUA's privacy practices. The process is described on the NCUA's privacy website. The Privacy team appropriately records and tracks complaints, concerns, and questions to ensure prompt remediation.

Maintenance and Use

The NCUA should establish administrative, technical, and physical safeguards to protect PII commensurate with the risk and magnitude of the harm that would result from its unauthorized access, use, modification, loss, destruction, dissemination, or disclosure.

The NCUA implements, documents, and tests security and privacy controls as required by applicable NIST and OMB guidance. Access controls are of particular importance with regard to protecting individuals' privacy. Records management, both keeping records for the required time frame and timely destroying or accessioning them, is also a key component of managing privacy risks.

Maintenance and Use		
1	*Which statement is most accurate?*	• NCUA owns the System.
2	*Who has access to PII in the system?*	• NCUA Employees • NCUA Contractors • Employees and/or Contractors of the Vendor-Provider • Other: SSAs have access only for their own state's CUs. Credit unions only have access to their own CU.
3	*Which roles have access to PII in the system?*	• Some System Users • System Administrators • Developers • Other: SSAs

Records Management		
1	*Which records retention schedule(s) will apply to this system?*	• NCUA Record Schedule - Program Records

Transparency

The NCUA should be transparent about information policies and practices with respect to PII, and should provide clear and accessible notice regarding creation, collection, use, processing, storage, maintenance, dissemination, and disclosure of PII.

The NCUA's transparency efforts include providing adequate notice to individuals prior to collection of their PII. The NCUA achieves this with Privacy Act statements, or privacy notices (the latter if the collection is not associated with a Privacy Act System of Records), and compliance with the Paperwork Reduction Act.[3] The NCUA also publishes Systems of Records Notices in the Federal Register and makes them available on the privacy page of the NCUA's website.

Transparency		
1	*Will any forms or surveys be used to collect the information?*	• No

SORNs		
1	*Is the information in the system retrieved by a personal identifier?*	• Yes
2	*Applicable SORN*	• NCUA-22

[3] See the Collection and Consent section above.

Accountability

The NCUA should be accountable for complying with these principles and applicable privacy requirements, and should appropriately monitor, audit, and document compliance. The NCUA should also clearly define the roles and responsibilities with respect to PII for all employees and contractors, and should provide appropriate training to all employees and contractors who have access to PII.

Compliance with the Fair Information Privacy Principles

As evidenced by this PIA (and the other information publicly available on the privacy page of NCUA's website), the NCUA is committed to achieving and maintaining compliance with the Fair Information Privacy Principles.

Roles and Responsibilities of NCUA Staff

As detailed in the NCUA Acceptable Use Policy and applicable Rules of Behavior, all NCUA staff are responsible for protecting PII from unauthorized exposure and for reducing the volume and types of PII necessary for program functions. Staff must protect all PII that they handle, process, compile, maintain, store, transmit, or report on in their daily work.

To protect PII, staff must use proper collection, storage, transportation, transmission, and disposal methods, must not access PII beyond what they need to complete their job duties, and must not disclose PII to unauthorized parties. Managers are also responsible for providing their subordinates with context-specific practical guidance about protecting PII.

All NCUA staff are required to review and acknowledge receipt and acceptance of applicable Rules of Behavior upon gaining access to the NCUA's information systems and associated data.

Failure to protect PII may result in administrative sanctions, and criminal and/or civil penalties.[4]

[4] 5 U.S.C. § 552a(i)(3); NCUA Computer Security Rules of Behavior.

Training

Together with the Office of Human Resources, the Privacy team ensures that new employees complete mandatory privacy training, and all existing employees and contractor employees complete privacy refresher training once every fiscal year. NCUA staff electronically certify acceptance of their privacy responsibilities as a part of annual privacy refresher training. The Privacy team keeps auditable records of completion of all mandatory trainings.

Analysis and Approval

This PIA was approved by or on behalf of the Senior Agency Official for Privacy. Below are additional details regarding the review and approval of the PIA.

Analysis and Approval	
Privacy Risk:	Acceptable
Approval Date:	September 9, 2022